Муниципальное бюджетное образовательное учреждение
дополнительного образования
«Усть-Ишимский Дом детского творчества»

ПРИКАЗ

14.03.2022 г Усть-Ишим № 29

О назначении ответственных

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», приказа ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Смирнову Анжелику Геннадьевну, заместителя директора, назначить ответственным, за организацию обработки персональных данных.

1.1. На время временного отсутствия (болезнь, отпуск и т.д.), ответственность за организацию обработки персональных данных, осуществление организационных и технических мероприятий по защите персональных данных и осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону №152-ФЗ от 27 июля 2006 г., и принятыми в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, и иным локальным нормативным актам, возложить на Мыринову Светлану Михайловну, секретаря.

2. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» (Приложение № 1).

3. Утвердить и ввести в действие Инструкцию администратора информационных систем персональных данных МБОУ ДО «Усть-Ишимский ДДТ» (Приложение № 2).

Контроль за исполнением приказа оставляю за собой

Директор Зарипова З.А. Зарипова

Приложение № 1
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.2022 г № 29

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ»

1.1. Инструкция ответственного за организацию обработки персональных данных в МБОУ ДО «Усть-Ишимский ДДТ» (далее - инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ» (далее - ДДТ).

1.2. В целях реализации настоящей инструкции используются следующие термины и их определения:

1.2.1. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.2.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.2.4. Средство защиты информации - программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.3. Настоящая инструкция утверждается приказом директора.

1.4. Изменения и дополнения в настоящую инструкцию утверждаются приказом директора.

1.5. Настоящая инструкция является локальным нормативным актом, регламентирующим деятельность Центра.

1.6. Срок действия настоящей инструкции не ограничен и действует до принятия новой инструкции.

1.7. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

2. Общие положения

2.1. Настоящая инструкция определяет функции, права и ответственность ответственного за организацию обработки персональных данных (далее - ответственный) в ДДТ.

2.2. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных, не исключает обязательного выполнения их требований.

2.3. Ответственный назначается приказом директора ДДТ.

2.4. Ответственный непосредственно подчиняется директору ДДТ.

2.5. На время отсутствия (болезнь, отпуск, пр.) ответственного, его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

– осуществляет внутренний контроль за соблюдением работниками, обрабатывающими персональные данные в информационных системах персональных данных (далее - информационная система) и без использования средств автоматизации требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– взаимодействует с уполномоченными органами государственной власти Российской Федерации, органами по аттестации, испытательными лабораториями по вопросам обработки и защиты персональных данных (при проведении государственного контроля и надзора, аттестации, сертификации).

– актуализирует перечень должностей работников, имеющих доступ к обработке персональных данных;

– актуализирует перечень работников, допущенных в помещения, в которых осуществляется обработка персональных данных;

– доводит до сведения работников, обрабатывающих персональные данные положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам их обработки, требований к их защите;

– организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей, чьи персональные данные обрабатываются в Центре, и осуществляет контроль за приемом и обработкой таких обращений и запросов.

4. Права

4.1. Ответственный имеет право:

– требовать от работников, обрабатывающих персональные данные, соблюдения установленной технологии их обработки и выполнения инструкций по

обеспечению безопасности информации;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, уничтожения персональных данных и технических средств, обрабатывающих персональные данные;

– требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– подавать свои предложения по, совершенствованию организационных и технических мер по защите персональных данных.

5. Ответственность

5.1. На ответственного возлагается персональная ответственность за качество выполняемых им функций по обеспечению защиты персональных данных.

5.2. Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей инструкцией.

Приложение № 2
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.22022 г № 29

ИНСТРУКЦИЯ
администратора информационных систем персональных данных МБОУ ДО «Усть-Ишимский ДДТ»

1.1. Инструкция администратора информационных систем персональных данных МБОУ ДО «Усть-Ишимский ДДТ» (далее - инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ» (далее - ДДТ).

1.2. В целях реализации настоящей инструкции используются следующие термины и их определения:

1.2.1. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.2. Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение,

предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.2.4. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.2.5. Средство защиты информации - программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.3. Настоящая инструкция утверждается приказом директора.

1.4. Изменения и дополнения в настоящую инструкцию утверждаются приказом директора.

1.5. Настоящая инструкция является локальным нормативным актом, регламентирующим деятельность Центра.

1.6. Срок действия настоящей инструкции не ограничен и действует до принятия новой инструкции.

1.7. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

2.Общие положения

2.1. Настоящая инструкция определяет функции, обязанности и права администратора информационных систем персональных данных (далее - администратор информационной системы) ДДТ.

2.2. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных, не исключает обязательного выполнения их требований.

2.3. Администратор информационной системы назначается приказом директора ДДТ.

2.4. На время отсутствия (болезнь, отпуск, пр.) администратора информационной системы, его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3.Функциональные обязанности

3.1. Администратор информационной системы выполняет следующие функции:

3.1.1. Управляет параметрами информационной системы:

- управляет заведением и удалением учетных записей пользователей;
- управляет полномочиями пользователей;
- поддерживает правила разграничения доступа;
- управляет параметрами настройки программного обеспечения;
- управляет учетными записями пользователей программных средств обработки персональных данных;
- оказывает помощь в смене и восстановлению паролей;
- управляет установкой обновлений программного обеспечения;
- регистрирует события в информационной системе, связанные с защитой персональных данных (события безопасности);
- поддерживает конфигурацию информационной системы (структуру, состав,

мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией;

- восстанавливает работоспособность программного обеспечения и технических средств информационной системы.

3.1.2. Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных:

- отказы в обслуживании;
- сбои (перезагрузки) в работе технических средств и программного обеспечения;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору персональных данных;
- иные события, приводящие к возникновению инцидентов.

3.1.3. Своевременно информирует ответственного за обеспечение безопасности персональных данных в информационной системе, о возникновении инцидентов в информационной системе;

3.1.4. Принимает меры по устранению инцидентов, в том числе:

- по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев;
- по устранению последствий нарушения правил разграничения доступа, несанкционированного доступа к персональным данным, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

3.1.5. Ведет учет пользователей информационной системы;

3.1.6. Принимает участие в деятельности по:

– подготовке, пересмотру, уточнению локальных актов по защите персональных данных;
– аттестации объектов информатизации.

4. Права

4.1. Администратор информационной системы имеет право:

– требовать от работников - пользователей информационной системы соблюдения установленной технологии обработки персональных данных и выполнения требований инструкций по обеспечению безопасности персональных данных;
– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств, входящих в состав информационной системы;
– требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования системы защиты персональных данных;
– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– подавать свои предложения по совершенствованию организационных и технических мер по защите персональных данных.

5. Ответственность

5.1. Администратору информационной системы категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения информационной системы в неслужебных (личных) целях;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

5.2. На администратора информационной системы возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования информационной системы.

5.3. Администратор несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей инструкцией.